CLAIMS

What is claimed is:

1. A multi-function peripheral device comprising:

a memory storing instructions which, when processed by one or more processors, causes the multi-function peripheral to perform the steps of

detect that a request for data to be analyzed for viral infection has been received over a network from a network device; and

in response to detecting receipt of the request, providing data from the multi-function peripheral device to the network device over the network.

2. The multi-function peripheral device as recited in Claim 1, wherein providing data from the multi-function peripheral device to the network device over the network includes providing one or more data files to the network device over the network.

3. The multi-function peripheral device as recited in Claim 1, wherein providing data from the multi-function peripheral device to the network device over the network includes providing configuration data to the network device over the network.

4. The multi-function peripheral device as recited in Claim 1, wherein the memory stores additional instructions which, when processed by the one or more processors, cause the multi-function peripheral to perform the steps of:

receive replacement data from the network device that has been disinfected; and

replace the data on the multi-function peripheral device with the replacement data.

5. The multi-function peripheral device as recited in Claim 4, wherein the memory stores other instructions which, when processed by the one or more processors, cause the multi-function peripheral to after replacing the data on the multi-function peripheral device with the replacement data, generate and send a confirmation message to the network device.

6. The multi-function peripheral device as recited in Claim 4, wherein the memory stores other instructions which, when processed by the one or more processors, cause the multi-function peripheral to, after replacing the data on the multi-function peripheral device with the replacement data, generate a report and either print the report at the multi-function peripheral or fax the report to another location.

7. The multi-function peripheral device as recited in Claim 1, wherein the memory stores additional instructions which, when processed by the one or more processors, cause the multi-function peripheral to perform the steps of:

receive a request from the network device for the multi-function peripheral to quarantine or delete at least a portion of the data that was sent from the multi-function peripheral device to the network device; and

in response to receiving the request from the network device to quarantine or delete at least a portion of the data that was sent to the network device, quarantine or delete the at least a portion of the data that was sent from the multi-function peripheral device to the network device.

8. A multi-function peripheral device comprising:

a virus protection process configured to, upon receipt of data by the multi-function peripheral,

examine the data to determine whether the data contains one or more unauthorized instructions; and

in response to detecting that the data contains one or more unauthorized instructions, perform one or more actions.

9. The multi-function peripheral recited in Claim 8, wherein the virus protection process is further configured to prevent the data from being stored on the multi-function peripheral.

10. The multi-function peripheral recited in Claim 8, wherein the virus protection process is further configured to generate and provide a notification that the multi-function peripheral received the data containing one or more unauthorized instructions.

11. The multi-function peripheral recited in Claim 8, wherein the one or more unauthorized instructions are unauthorized executable program code.

12. A multi-function peripheral device comprising:

a virus protection process configured to, prior to sending data from the multi-function peripheral to a network device over a network,

examine the data to determine whether the data contains one or more unauthorized instructions; and

in response to determining that the data contains one or more unauthorized instructions, perform one or more actions.

13. The multi-function peripheral recited in Claim 12, wherein the one or more actions include not sending the data to the network device.

14. The multi-function peripheral recited in Claim 12, wherein the one or more actions include generating and providing a notification that indicates that the multi-function peripheral has the data that has been infected by a virus.

15. The multi-function peripheral recited in Claim 12, wherein the one or more unauthorized instructions are unauthorized executable program code.

16. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is configured to detect that one or more unauthorized instructions have been stored on the multi-function peripheral by examining and detecting that the data has been modified.

17. The multi-function peripheral device as recited in Claim 12, wherein the data is stored on a non-volatile memory of the multi-function peripheral.

18. The multi-function peripheral device as recited in Claim 12, wherein the data is stored in a volatile memory of the multi-function peripheral.

19. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to undo changes made as a result of execution of the one or more unauthorized instructions.

20. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to

determine whether the data stored on the multi-function peripheral can be restored to a prior state; and

in response to determining that the data cannot be restored to the prior state, then delete the data from the multi-function peripheral.

21. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to render the data inaccessible on the multi-function peripheral.

22. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to notify a user via a graphical user interface on the multi-function peripheral that the data contains one or more unauthorized instructions.

23. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to notify a user by printing a report on the multi-function peripheral that indicates that the data contains one or more unauthorized instructions.

24. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to provide notification via an email that the data contains one or more unauthorized instructions.

25. The multi-function peripheral device as recited in Claim 12, wherein the virus protection process is further configured to provide notification via a facsimile that the data contains one or more unauthorized instructions.

26. The multi-function peripheral device as recited in Claim 12, wherein the multi-function peripheral is configured to receive, over a network, data used by the virus protection process to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral.